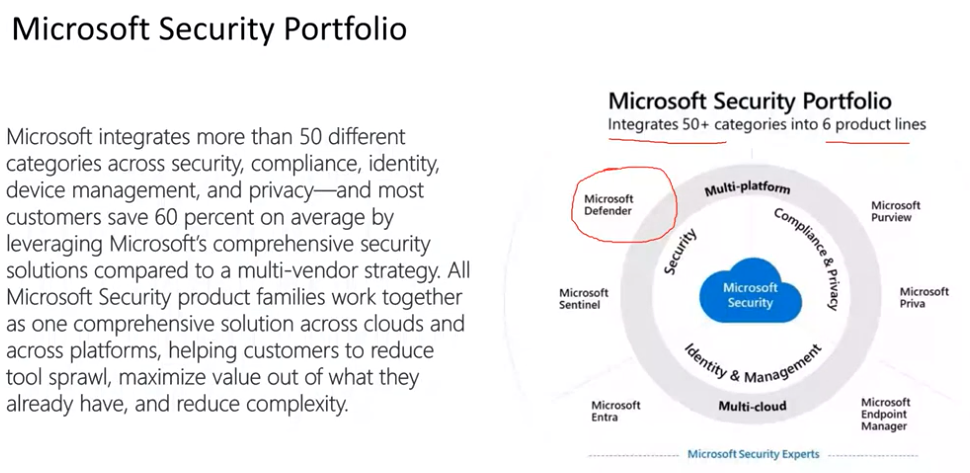
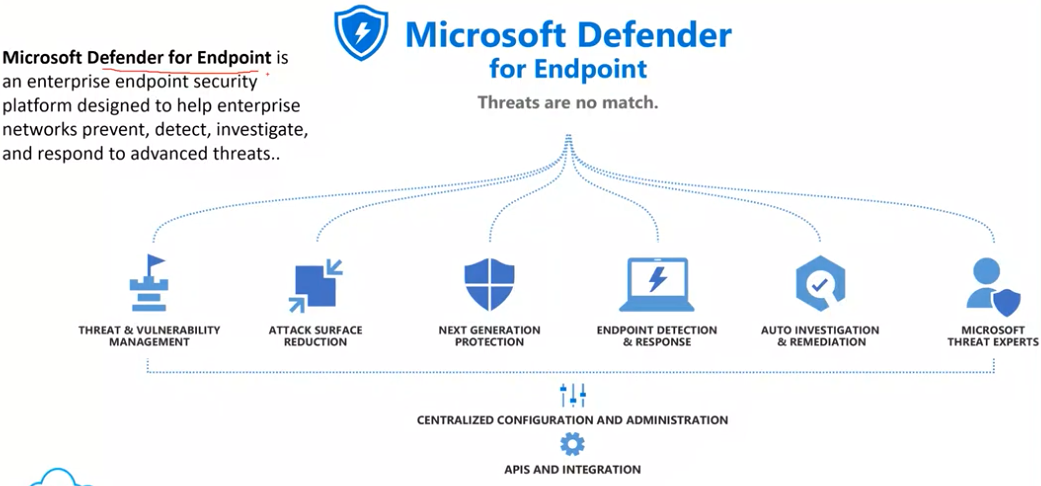
Microsoft Defender for Endpoint security

Extracted from [here](https://www.youtube.com/watch?v=zsUKA4iCCGM&list=WL&index=17&t=1s):

For management tools the settings for enterprise can be centrally maintained by using either Grow Policy, System Center or Ms Endpoint manager.



Microsoft Defender itself consist of Endpoint, cloud apps, IoT, and more.



In threat and vulnerability management there are 2 scores exposure score (lower the better), Device security score (the more the better).

Attack Surface Reduction; allows 16 different rules (in each rule we can like block or allow certain things e.g. disabling macros for office products means disabling child processes like running a powershell script on a macro to control a device or whatever).

Next Generation Protection is basically a antivirus.

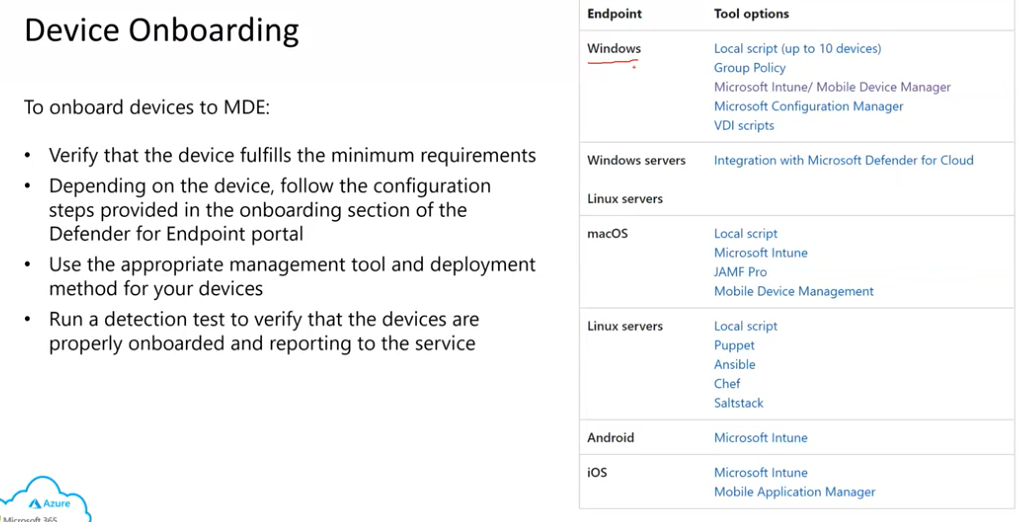
Endpoint Detection & Response works in close with above, its based on behavioral monitoring. EDR is best as it also provide means for file-less attacks. In video a case was represented, the person closed the NGP and initiate attacks the EDR was able to log those and prevent those.

Auto Investigation; it helps the admin to automate the alerts system (for each alert do auto investigation and stuff). Because in enterprise application in each second hundreds of logs are generated.

# ASR 16 Rules

# 

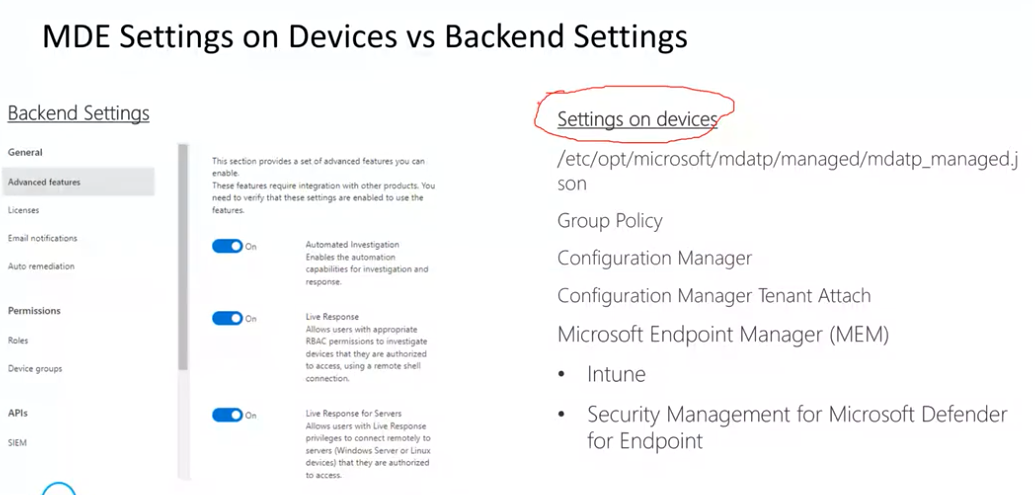
# Step 1:



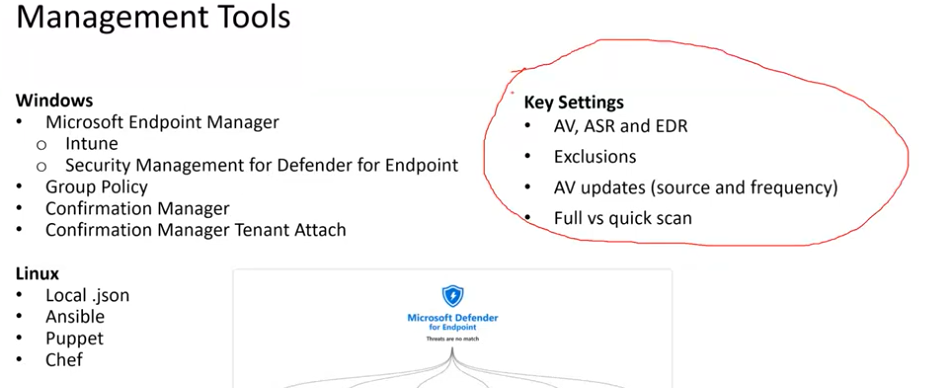
In Device Invetory you can see all listed devices, in settings -> endpoints -> onboarding you can have steps to onboard a device.

# Step 2 (could be 1):

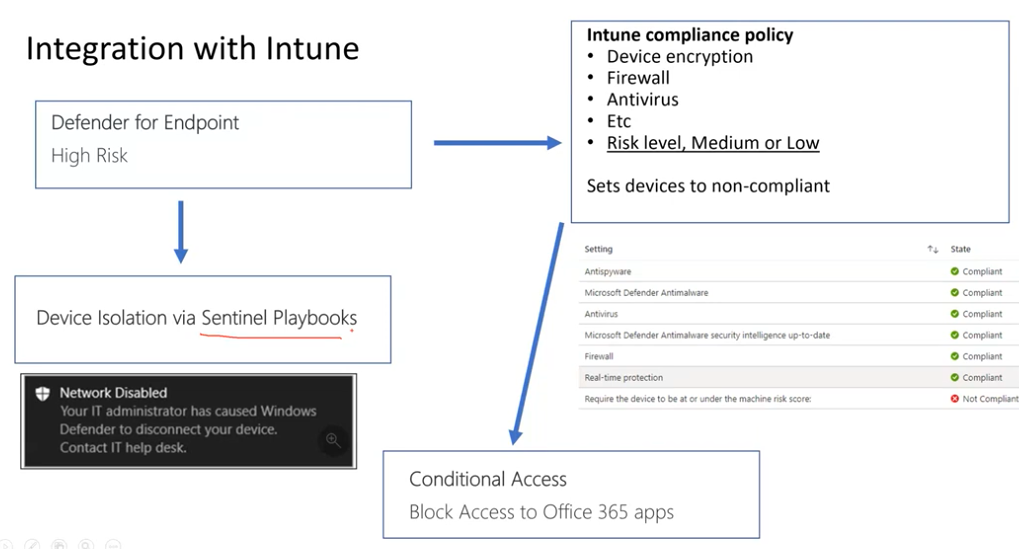
Configuring settings:

Backend settings from security.microsoft.com, Device settings from endpoint.microsoft.com

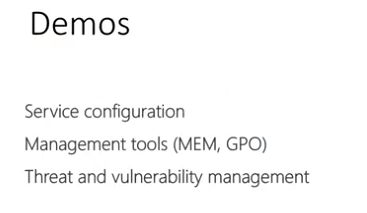
Important Backend settings: advanced features, device groups, indicators (control whitelist and blacklist or file hashes, ips, URLs and certificates).



Exclusion is like if your running a heavy system like oracle`s heavy database and then avoid the investigation of every single request/transaction by excluding oracles stuff. AV updates get after every 4 hours or 6 hours.



Sentinel is the SIEM solution so in case of an attack the attacker can exploit network from this high risk device so to avoid it till the time sentinel is talking to defender the device is removed from network completely.



Threat and vulnerability management demo from [50:04](https://youtu.be/zsUKA4iCCGM?si=MG-zxAJXo-JddSxQ&t=3004),